2005

Unsolicited Commercial Email (SPAM): An Exploratory Understanding Using Stakeholder Analysis

Evangelos Moustakas
Middlesex University - U.K., e.moustakas@mdx.ac.uk

C. Ranganathan
University of Illinois at Chicago, ranga@uic.edu

Penny Duquenoy
Middlesex University - U.K., p.duquenoy@mdx.ac.uk

UNSOLICITED COMMERCIAL EMAIL (SPAM): AN EXPLORATORY UNDERSTANDING USING STAKEHOLDER ANALYSIS

Evangelos Moustakas, Middlesex University, NW4 4BT, The Burroughs, Hendon London UK, e.moustakas@mdx.ac.uk.

C. Ranganathan, University of Illinois at Chicago, 601 S Morgan Street, Chicago, IL-60607, USA, ranga@uic.edu

Penny Duquenoy, Middlesex University, Trent Park R7, London, UK. p.duquenoy@mdx.ac.uk.

Abstract

The growth in the use of email marketing has been accompanied by an enormous increase in the amount of Unsolicited Commercial Email (UCE), popularly known as spam. The unprecedented amount of unsolicited messages is now recognized as a serious problem, costing the society billions of dollars very year. In this paper, we provide an exploratory understanding and conceptualization of unsolicited commercial email. Based on critical characteristics of UCE, we propose a conceptual typology of spam. Further, we identify the key stakeholders in the UCE process and enunciate the roles played by them. Using the stakeholder analysis, we highlight some key mechanisms for addressing the problem of UCE.

Keywords: Unsolicited commercial email, spam, Internet marketing, Stakeholder analysis, electronic mail.

1. INTRODUCTION AND MOTIVATION

Internet offers a cost effective medium to build better relationships with customers than has been possible with the traditional marketing media. Internet technologies such as electronic mail, web sites and digital media offer companies the abilities to expand their customer reach, target specific communities and communicate as well as interact with customers in a highly customized manner. In the last few years, electronic mail has emerged as an important marketing tool to build and maintain closer relationships with customers as well as prospects. Email marketing has become a popular choice for several companies as it greatly minimizes the costs associated with other conventional methods such as direct mailing, cataloging and telecommunication marketing.

The growth in the use of email marketing has been accompanied by an enormous increase in the amount of Unsolicited Commercial Email (UCE), popularly known as *spam*. The unprecedented amount of unsolicited messages is now recognized as a serious problem, costing the community billions of dollars very year. The problem of spam extends beyond household Internet users to the realm of companies as many precious employee hours are being wasted due to spam messages. Gartner estimates that over 50% of email messages received by an average firm constitute spam (Gartner 2003). According to Sophos, a corporate spam and antivirus company, global spam messages in 2004 was over 3 trillion, costing over 131 billion US dollars (Coroneos, 2004). Jupiter Media Metrix estimates that each piece of spam costs $1 in lost productivity (Shiels, 2002). According to Ferris Research, approximately an average employee wastes $4,000 a year dealing with spam, cumulating to over $10 billion in 2003 (Krim, 2003). Spam results in wastage of time, effort, disk space, in addition to consuming network bandwidth and affecting critical technology resources. While higher amount of spam could force individuals to spend more time sifting through their messages resulting in increased usage costs, the transmission costs incurred by Internet service providers due to spam could result in added service charges for customers.

As email has emerged as a major means of personal and corporate communication, there has been increased academic focus on the usage and impacts of email. Researchers have studied richness of communication using emails (Lee, 1994; Ngwenyama and Lee, 1997) individual perceptions concerning email (Higa et al., 2000; Hoxmerier and Nie, 2000; Pendarkar and Young, 2004), impact of email on work practices and employee productivity (Jackson et al., 2003) and intra-organizational and inter-organizational impacts of email (McManus et al., 2002). However, there is only limited academic literature on unsolicited emails. While the importance of studying spam is well recognized (Sipior et al., 2004), empirical research on spam has been limited and still emerging. In fact, calls have been made for a better understanding of electronic mails and their impacts on individuals and corporations. Weber (2004), in his editorial statement of *MIS Quarterly* remarked: “both the professional and personal impacts [of emails] on us have been profound, yet our understanding of these impacts remains fragmented and superficial. Similarly, I feel we lack a good understanding of the impacts of e-mail on groups and organizations” (p. iii).Our paper is a preliminary effort in response to this research call.

For rigorous empirical research and theory building on UCE, some basic understanding and conceptual foundations are critical. Recognizing this concern, our paper provides some exploratory understanding and conceptualization of unsolicited commercial email. Our research objectives are three fold:

- *(i) To provide a conceptual overview of the UCE process*
- *(ii) To propose a typology of UCE, and*
- *(iii) To delineate key stakeholders of the UCE, their roles and potential responses through a stakeholder analysis.*

2. WHAT IS UCE?

The term `spam' was initially used in the monty python skit (Monty Python sketch, 1970) in which the spam meat product was featured. In this skit, a group of Vikings sang a chorus of "spam, spam, spam ..." in an increasing crescendo in a restaurant where everything on menu included spam. Like the song, spam it is commonly used to describe unsolicited, often bulk e-mails (Langford, 2000, p.23). According to Turban et al. (2000) spam or UCE is defined "as the practice of indiscriminate distribution of messages without permission of the receiver and without consideration for the messages' appropriateness" (p.360). These definitions consider the permission from receiver, and the quantity of mails sent to describe UCE. The Direct Marketing Association's definition reflects both these characteristics: "The act of sending unsolicited bulk commercial e-mails to an individual's e-mail address without having an existing or prior business/personal relationship or obtaining consent/permission" (DMA, 2003). These definitions of spam take a recipient perspective, without taking into consideration the sender. However, UCE includes the term "commercial", reflecting the goal of sender - it implies a commercial intent such as advertising, marketing or promotion. In this paper, we are primarily concerned with unsolicited communications that have a commercial intent. UCE is different from other unsolicited emails such as chain letters containing jokes and religious promotion material etc. The growth of UCE and its variants have resulted in non-commercial, malicious outcomes as well. Several UCE messages serve as carriers and distributors of viruses that could potentially be harmful to recipient.

Given the evolution of spam and its changed characteristics, UCE could be categorized into multiple types:

- Junk e-mail - Bulk sending of unwanted commercial e-mailing
- Non-Commercial Spam - Bulk sending of unsolicited e-mailing without commercial interest such as chain letters.
- Offensive Spam – Bulk sending of mailings with 'adult' oriented content i.e. pornography.
- Spam Scams **–** Bulk sending of fraudulent mailings with the intention to invade the privacy of the recipient.
- Malicious **–** Mass mailings that contain malicious programming code such as Viruses and Trojans.

Based on the content of spam, Federal Trade Commission (FTC, 2003) classified UCE into the several categories (Table.1). The issue of UCE spans a number of Internet user groups ranging from online users and internet-service providers and policy makers. According to Erkki Liikanen, European Commissioner for Enterprise and the Information Society, "Combating Spam has become a matter for us all and has become one of the most significant issues facing the Internet today" (Liikanen 2003).

Content	**Description**
Investment/Business Opportunity	Work-at-home, franchise, chain letters
Adult	Pornography, dating services, etc
Finance	Credit cards, refinancing, insurance, foreign money offers, etc
Products/Services	Products and services, other than those coded with greater specificity
Health	Dietary supplements, disease prevention, organ enlargement, beauty products including weight loss drugs
Computers/Internet	Web hosting, domain name registration, email marketing
Leisure/Travel	Vacation opportunities
Education	Diplomas, job training
Other	Types of offers not captured by specific categories listed above

Table.1. Types of UCE

While UCE serves as a low-cost marketing tool for senders, it poses a serious threat to the privacy of individual Internet users (Meade, 2003). The practice of spamming, and in particular the way in which e-mail addresses are collected or sold, raises a number of additional concerns. Techniques such as phishing (ie., creating fake identities using spoofs of well-known names) that fool the user into providing personal information such as financial data, account numbers and passwords have become increasingly sophisticated (Graham, 2004). A significant proportion of UCE contains fictitious information about the sender, misleading subject lines or performance claims, advertisements for pornographic web sites, software offers for collecting email addresses, quack products and illegally pirated software. Therefore, the problem of UCE poses a fundamental threat to e-commerce.

UCE also burdens internet-service providers (ISPs) who bear much more of the cost of providing the infrastructure. Spam consumes resources such network bandwidth, storage space, and computing power, causing significant performance issues for ISPs as well as their clients. Several systems have collapsed due to the sheer bulk of spam. Moreover it creates support overheads for ISPs who must deal with spam complaints from their customers.

Lost productivity is another negative effect of spam (Khong, 2004). When employees receive UCE at work, their work time is spent in reading, responding to deleting messages. Organisations need to examine what percentage of their labour costs are lost due to employee time spent on junk mails, apart from the additional workload to their data centre and MIS staff. There are other productivity drains as well: on legal front, there have been instances of lawsuits as a result of pornographic and other messages circulated via email in the workplace. Junk email not only costs corporations dearly in precious network resources and employee productivity but also carries with it serious legal liability as well as network security risks.

UCE is also increasingly used as a vehicle for spreading computer viruses and worms. Spam and e-mail-born viruses can no longer be treated as separate problems. More than 98% of computer viruses now arrive via spam**,** cleverly camouflaged with spooky message headers. Spam, which most frequently takes the form of mass mailing advertisements, is a violation of Internet etiquette.

3. A TYPOLOGY OF SPAM

Based on the definitions and characteristics of UCE identified from prior literature, two distinct characteristics of UCE emerge as being salient – (i) the origin of UCE, whether the email was an outcome of an intended or unintended action of the recipient. The intended actions include voluntarily providing email address to some web sites or online stores or while performing some online or offline transaction. Here, the user had explicit knowledge that the email address is being given out, as he/she initiated such an action. On the other hand, the email address could also have been compiled by a third party without the explicit knowledge or consent of the recipient. (ii) the extent of negative impacts of the UCE. The consequences of a UCE could vary from being useful to a recipient, to causing minor disturbance to much negative outcomes such as a virus attack and related consequences. As UCE is largely considered to be negative in nature, we focus on the extent of potential negative impacts. Based on these two dimensions, we propose a typology of UCE that delineates four types (Table.2). Our approach is consistent with Khong (2004) who categorized spam into those that relate to ` contract offer' and those that are `nuisance'. These four types are described below:

Origin	Low	High
Third-party initiated	II	IV
Self-Initiated	I	III

Potential Negative Impact

Table.2. Proposed Typology of UCE

Type I: This type of UCE represents a direct relationship between the sender and recipient. The relationship assumes some degree of legitimacy as the recipient provides explicit consent to receive direct e-mail marketing. This consent could through web forms, email requests or through other explicit means of subscription (opt-in methods). Typically, there is a provision to opt-out of the relationship as the recipient could request termination of communication at any point in time. An important characteristic of Type-I UCE is that the identity and contact details of the sender are known to the recipient. In USA, a sender could send UCE without explicit consent of receiver, and this action would be considered legitimate provided the sender fulfils some basic requirements such as revealing his identity, contact details and providing a way for recipients to opt-of the communication. Some states in USA mandate marketers to use the term "ADV" in the subject line of the messages to explicitly declare that the mail is marketing-related.

Type II: This type of communication can be described as an indirect, permission-based partnership. When consumers complete some kind of on-line transaction, they are asked to opt-in to certain e-mail lists of related services or affiliates. Information about consumers is sent to affiliates and other third parties who initiate communication with the recipients. The consumers may not be aware of these third parties at the time of providing their permission. Several direct marketing associations also maintain mailing lists of consumers who had provided them with their contact information. Typically, the consumers could request termination of communication as well.

Type III: This category includes spam that originates from third parties without explicit permission or consent of recipients. Email databases compiled from public domains and free email services, and web-sites with non-secure transmission of personal information through on-line forms typically serve as primary sources of consumer contact information. Sometimes, spammers employ search bots that navigate the Internet and automatically retrieve e-mail addresses from public areas. Sometimes, they also forge the headers of their email in an attempt to avoid losing their accounts and to evade email filters. Several offensive spam fall under this category. The opt-out links at the bottom of spam mail may not work, and, rather they are used to verify the validity of the recipient's email address.

Type IV: In this category, the identity of senders is unknown and the intention of the spammers extends beyond simple commercial purposes to being potentially harmful to the recipients. Spammers could implant viruses, spy code, malicious software, or other potentially damaging tools in the email that could harm the recipient. Sometimes, the malicious code could stay inside the recipient's computer, intruding into the privacy, retrieving information about the recipient and sending it back. In many cases, the consumers may not even be aware of the presence of the malicious code, and have little knowledge of them.

4. STAKEHOLDER ANALYSIS

Stakeholder analysis has become an established framework to identify and examine the interactions between organizations and constituents in external environment. It was originally advocated by Freeman (1984) as a tool for managers to proactively engage their external environment in the face of a rapidly changing global marketplace. The term ‘stakeholder’ refers to individuals, groups or organizations that need to be taken into account by leaders and managers contemplating any action on an issue. While earlier researchers confined stakeholders to a firm based on their organizational membership, subsequent scholars have recognized the existence of stakeholders outside of firm boundaries. Mitchell et al (1997) suggested a framework for stakeholder identification based on three criteria namely power, legitimacy and urgency. Stakeholder analysis has been widely applied in strategic management, corporate governance (Burgoyne, 1994; Donaldson and Preston, 1995) as well in information systems studies. Following DAvindson and Preston (1995) and Mitchell et al (1997), we extend the stakeholder analysis to the context of UCE. Through this analysis, we seek to identify salient stakeholders, their position and potential roles in the UCE process.

Figure 1 provides a pictorial representation of the UCE process and the key stakeholders in this process. As shown in the figure, there are four primary groups of stakeholders. First, the category 'senders’ serves as the originator of spam and includes corporations, direct marketers, and a host of other illegitimate Spammers. Second, at the receiving end are individuals and online users. Third, a group of intermediaries intervene in the UCE process to directly or indirectly control, manage and co-ordinate the process. This category includes (i) internet service providers (ISPs) who typically deploy anti-spam tools, and/or email usage policies for their customers, (ii) direct marketers associations (DMA), who co-ordinate and control their members’ communication behaviour through their codes and policies and (iii) consumer privacy associations. Fourth, the final group consists of government bodies that oversee and regulate the UCE process.

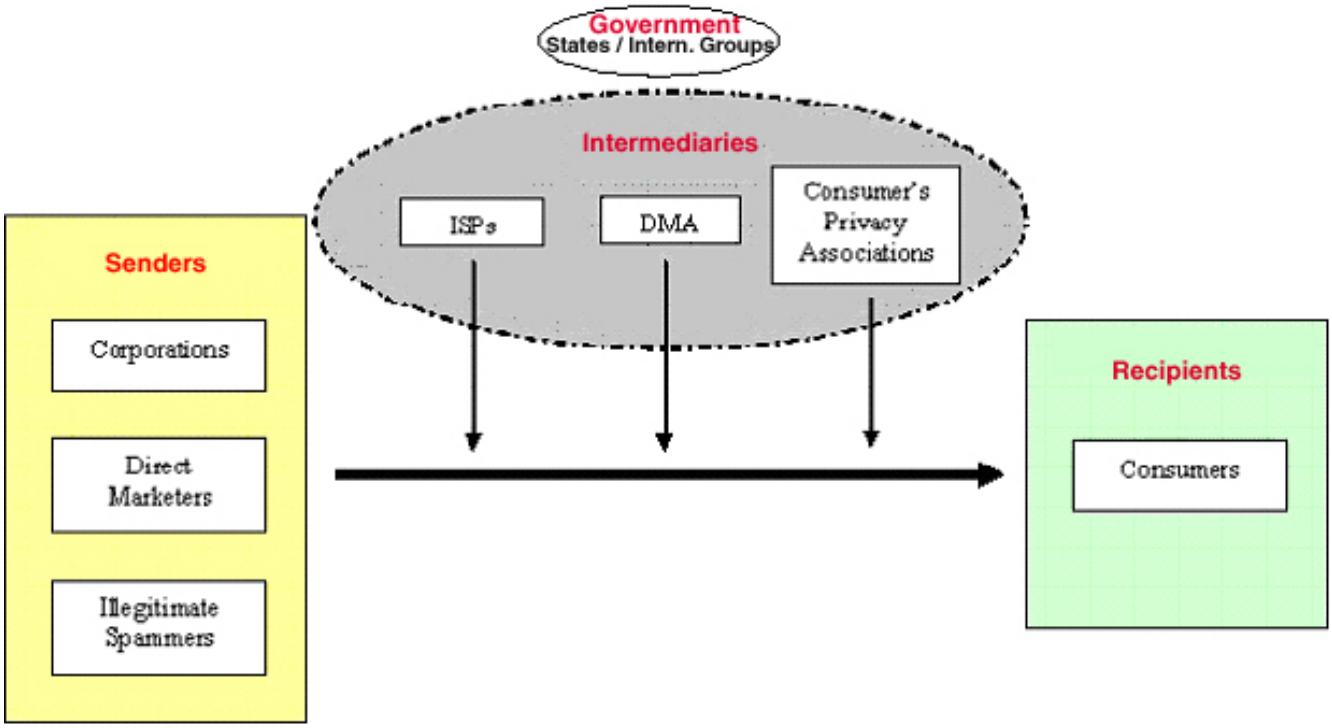

Figure.1. UCE process and key stakeholders

Senders of UCE:

Corporations: One of major factors that make email marketing an attractive proposition for senders is the low marginal costs for sending bulk emails. Several corporations solicit their customer's email addresses to send them promotion and other material. Corporations use these emails to conduct targeted campaigns, distribute material such as discounts and coupons, and for general promotional purposes. Another positive attribute of email marketing concerns the affordability by small and medium sized businesses who are constrained by resources for conducting large marketing or promotional campaigns. An argument that has been floated in favour of email advertising is that this represents a significant economic opportunity for small and medium enterprises and it should not be undermined by restrictive regulations.

Direct marketers: This group is engaged in the business of direct marketing. They maintain customer contact databases and engage in commercial communication on behalf of other merchants and marketers. The customer contact information is usually solicited or collected by the direct marketers. Many corporations and marketers tend to outsource their email communication or part of their promotional campaigns to these direct marketers, who provide email and other direct marketing services for a few. For direct marketers, the low costs of email marketing are extremely attractive because even low response rates could result in some profits.

Illegitimate spammers: Illegitimate spammers include those who send emails without any prior consent of recipients. They collect email addresses from various on-line resources such as newsgroups, online directories, web-pages and use them for sending commercial emails. They claim that email addresses are as public as phone numbers. If someone does not want to receive junk email he should not place his address anywhere that is publicly accessible. Relying on tools such as automatic harvesting programs and dictionary attacks, spammers have developed a number of ways to collect e-mail addresses. In addition, by relying on technical measures such as false headers, mail relays, and spoofing, spammers can hide their identities making them difficult to locate.

Receivers of UCE:

Consumers: The major motivator for individuals to opt-in to e-mailing lists is the anticipation of receiving relevant material that matches their interests. Individuals tend to value the relevance of promotional messages (Grunert, 1996; Gengler and Reynolds, 1995). Opted-in customers are free to unsubscribe or leave the listing at any time. However, if the real problem arises when individuals are targeted for UCE in which they have no interest or relevance. Large volumes of commercial e-mail communication tend to irritate individuals due to the fact that they are forced to spend their time and effort in downloading, reading, or deleting spam. Krishnamurthy (2000) listed seven reasons when UCE could become an unethical communication practice – violation of privacy, volume of emails that consumes time and effort, irrelevance of communication received, deceptiveness of emails (forging sender identity or message title), offensiveness and targeting vulnerable customers. Individuals' privacy cost is a major factor that raises serious concerns about the privacy of the information that they provide to companies and marketers. Finally, individuals tend to favour mailing lists that have clear and reliable opt-out opportunities.

When individuals receive spam at work, it creates problems for the corporations as well. Enterprises play a double role in the UCE process. When employees are targeted for UCE, the precious server space and bandwidth of the corporate IT infrastructure gets wasted. Moreover, the problem of dealing with spam rests in the shoulders of corporations as these pose a threat to the employee productivity as well as security and privacy of corporations. While most firms do not wish to receive any unsolicited email communication from third parties, but most of them use email as a marketing tool. Firms need to invest in anti-spam tools to control incoming spam, but should also need to create a delicate balance about their own email marketing campaigns.

Intermediaries:

Internet Service Providers (ISPs): An important stakeholder in the UCE process is the ISP, who provides the fundamental internet access services to both senders as well as recipients. Internet Service Providers have become a critical component of the commercial Internet providing customers Internet access, web hosting services, e-commerce technologies, and email access. According to the Electronic Commerce (EC Directive) Regulations 2002, ISPs are 'mere conduits' and as a result are not liable for the content of information they transmit through their networks. There is a general argument that ISPs need to be the first line of defence in combating spam. The Internet Engineering Task Force's (IETF) Network Working Group has developed protocol standards (RFC 2871) and best practices (RFCs 2505 and 2635) for ISPs to follow in order to help reduce spam. These standards require ISPs to prevent their mail servers from being used by unauthorised third parties to relay e-mails and to provide sufficient information in e-mail headers to make it possible to verify the source of e-mail.

Direct Marketing Associations: Associations of direct marketers are also trying to control their members' behaviour online (DMA, 2002). But even effective self-regulation by such bodies could be ineffective as many several spammers may not be members of the organisation. For instance, The Canadian Marketing Association (CMA) has established for its members a code and guidelines dealing with Internet use for the distribution of promotional materials. Under this code, consumers who are solicited must be given the opportunity of "opting-out" of any further communication from the marketer. A marketer who fails to live up to the CMA code is expelled from the Association.

Consumer Privacy Associations: Their role is to provide education and awareness-raising programs to empower consumers to make informed choices in relation to spam reduction strategies and technologies. For example the 'Korean Information Security Agency' has set up a black list of spammers and the 'Union Fédérale des Consommateurs de Quimper' in France provides information on existing spam-related laws and how to take legal action against spammers. In other occasions, they operate as reporting centres that receive complaints on spam, and analyse or forward the spam to the appropriate authorities for further investigation.

Government / State: More and more countries have laws in place that directly or indirectly regulate spam. Anti-spam laws generally impose labelling requirements, prohibit the transmission of commercial communication without the consent (opt in/out) of the recipient and ban the use of 'spamware'. Examples of regulations across the globe include the Canadian Code of Practice for Consumer Protection in E-Commerce, the US CAN-Spam Act of 2003 for Unsolicited Commercial Electronic (UCE) Mail and other similar regulations by European Union, EU Directive 2002/58. The legislations usually relate to a number of issues:

- Breach of Contract with the ISP: the spammer may breach the terms and conditions of his ISP by sending bulk UCE.
- Trademark Infringement: forged headers – (e.g. AOL trademark)
- Computer Misuse Act: malicious programming code integrated within the e-mail
- Data Protection Act 1998: impingement on personal information. A data controller (in this case spammer) must process data fairly and lawfully. An individual who suffers damage as a result of a breach of this requirement can ask for compensation.
- Consumer Law: Deceptive on-line offers and insecure e-commerce environment

5. MECHANISMS FOR TACKLING UCE

In UCE, the most affected parties are the consumers. Customer pressure could be powerful force that could go a long way in containing and eliminating spam. The customer pressure for better online services including spam free email communication will force ISPs to develop anti-

spamming software applications and enforce constructive email policies. If ISPs do not comply, they will face the danger of being excluded from the market by customers.

There are a number of actions individuals can take when receiving UCE.

1. Disregard and delete – Simply delete the message. This is an acceptable solution as long as the amount of spam is small. However, it is not a recommended method when spam reaches a high rate.
2. Block and delete – This is a more effective method since blocking will not allow further receipt of communication from the same source. However, it contains the danger of legitimate e-mail to be wrongly blocked.
3. Quarantine - There are several anti-spamming software that quarantine suspicious e-mail (potential spam) and put it on a separate folder for further inspection.
4. Report – Report all spam messages to the appropriate authorities (ISPs or potentially the Police) although it may not lead to the identification of the sender of the e-mail (spammer).
5. Respond – There are cases where the commercial e-mail message is coming from a known source or from a trusted third party and then we may read it, download an attachment or even reply. Although it is not recommended, individuals may receive commercial communication that is close to their interest and as a result to open the message.

Table.3 presents our initial typology of UCE, along with key stakeholders in each category and possible response mechanisms for minimizing spam.

Third-party initiated	**Key Stakeholders** **II** DMA ISPs **Potential responses** Enforcing code of conduct by DMAs. Email usage policies and filtering solutions by ISPs.	**Key Stakeholders** **IV** Government ISPs **Potential responses** Anti-spam legislations. Penalties for non-compliance with legislation.
Self-initiated	**Key Stakeholders** **I** Consumers Corporations **Potential responses** Consumer opt-in; opt-out Explicit policies by corporations	**Key Stakeholders** **III** DMA ISPs Consumer's Privacy Associations **Potential responses** Enforcement of stringent code of conduct by DMAs. White and Black listing by ISPs. Promote consumer awareness on privacy issues.
	Low	***High***

Potential Negative Impact

Table.3 Mechanisms for containing UCE: Stakeholders and Potential Responses

Type I: This type of UCE is relatively easier to manage and control. The key stakeholders in this type of communication are customers and corporations. The UCE here is similar to the idea of 'permission marketing' (Godin, 1999), where explicit permission of customers is sought before communication is sent to them. Along with permission, possible compensation, rewards, volume and targeting are also considered (Milne and Gordon, 1993). Consumers could opt-in or opt-out of UCE, or they could use software tools to monitor, delete or respond to this communication.

Several corporations who collect customer email ids have explicit policies in place that specify the purpose of collecting the contact information and how this information will be used.

Type II: The key stakeholders here are DMA and ISPs as this kind of UCE is third-party initiated, rather than customer-initiated. DMA forms an umbrella-organization for most direct marketers who are governed by code of conduct and norms prescribed by DMA. DMA's interest lies in protecting the efficacy of email marketing as a promising and cost-effective marketing medium. Another important stakeholder group who can play a critical role in minimizing this type of UCE is the ISP who can adopt stringent measures regarding those responsible for sending and propagating spam. ISPs represent a fairly large industry across the globe, and the policies adopted by ISPs vary considerably across the globe. While some ISPs might be more effective in controlling the spam, others may not have stringent measures in place. ISPs could enforce strict anti-spam policies for its members, in addition to deploying anti-spam filleting solutions.

Type III: This category includes cases where customer opt-out mechanisms are not effective or cases where the email lists have been passed on to different parties with or without explicit knowledge or consent of the customer. The key stakeholders who can be effective in controlling this type of communication are DMAs, ISPs and Consumer Privacy Associations. DMA could ensure member compliance with rules and norms on information sharing, and such code of practice. ISPs set-up and maintain black/white lists that control the flow of email communication. The purpose of a white list is to specify elements whose inclusion in an e-mail guarantee it will pass the filter and be delivered. On the other hand, inclusion in black list blocks the passage of email. Consumer's Privacy Associations provide educational programs and awareness campaigns to empower customers to make informed choices in relation to spam reduction strategies and technologies. The also operate reporting centres that receive complaints on spam, and analyse or forward the spam to the appropriate authorities for further investigation

Type IV: This represents the most dangerous form of UCE where very little is known about the origin of the UCE, with potentially high negative impacts. While a number of technological solutions in the form of advanced filtering tools, anti-spam and anti-virus solutions have become available in the marketplace, none of them have been completely successful in eliminating spam. We identify the key stakeholders in this type of communication as the ISPs and governments at a global level. While ISPs can effectively implement sophisticated technological solutions, governments could propose and enact different anti-spam legislations to combat UCE. The legislations deal with issues such as prevention, consumer's awareness, reporting mechanisms, remedies and penalties, cross border complaints, international cooperation and monitoring.

Arguments have been made for and against legalizing UCE through legislation. CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) act in USA requires that spam e-mails include a working return e-mail address, a valid postal address for the sending company, a working opt-out mechanism, and a relevant subject line. This law does not prohibit senders from sending spam messages until customer explicitly asks to be opted-out. CAN-SPAM is an "opt-out" legislation that puts the onus on individual users to let marketers know that they do not wish to receive UCE. In contrast, European Union (EU) and UK use "opt-in" legislation where online marketers can send UCE messages only to those consumers who have given their prior consent to receive them, except where users are current customers of a particular company (EU Information Society, 2003)

There are also differences in interpretations of regulations across nations and even within groups such as EU. While some impose fines for unsolicited e-mail sent to both customers and businesses others only penalise spam sent to customers. There are a number of differences even among the EU member states in areas such as nature of consent (oral or written); explicit or

implicit; active versus passive; and the authorities who would manage the opt-in/opt-out lists. Spain takes the view that messages can only be sent to those who have authorised them, but Denmark has banned the sending of messages unless the recipient has actually requested them. In the UK, participation in a draw would constitute consent to receive further e-mails. Though harmonization of laws across a larger group of nations worldwide is a formidable task, efforts are in progress towards achieving this larger goal.

Apart from legislation, there are several steps that could be taken by corporations and individuals to combat UCE. One of the key steps that businesses can adopt is development of an e-Policy that clearly details how spam is handled. Guidelines about subscribing to email newsletters and web-sites that require an email address are critical. E-Policies also need to specify how employees should handle unsolicited email, especially if the email contains offensive material. In addition, the e-Policy should detail how employees can use email for personal use. Ensuring that employees understand and acknowledge e-Policies is necessary. A well-structured email policy, along with educating the employees and enforcing compliance with the formulated policies using technological tools can go a long way in combating UCE in workplace. Increasing consumer awareness globally is another key measure that could help address the problem of UCE. Consumers need to be aware of their rights, privacy issues and mechanisms through which they can combat spam.

6. CONCLUSIONS

While email has emerged as a powerful marketing tool, the cost-effective capability of email has also given rise to the problem of unsolicited commercial communication. In this paper, we undertook an exploratory analysis of UCE process. We proposed a typology of UCE, identified key stakeholders in the process and also highlighted some key mechanisms for addressing the problem of UCE.

UCE has become a global problem requiring a global solution. As e-mails can originate or be routed through servers around the world, collaborative cross-national efforts to investigate and prosecute spammers have become a necessity. Increased consumer and industry awareness, development of corporate e-policy practices, stringent code of conduct for direct marketers, sophisticated email monitoring and blocking by internet service provides and enforcement of strict legislations education are some of the key mechanisms to combat the problem of UCE. No single mechanism addressing the problem of spam -- neither technical nor regulatory in nature is likely to be successful on its own. A unified effort, combining all the key stakeholders in the UCE process, will be the most effective way to combat and manage spam.

References

Burgoyne, John G., Stakeholder analysis, in Cassel. C. and G. Symon (ed.), Qualitative Methods in Organizational Research: a practical guide, Sage, New Delhi, pp. 187-207, 1994

Coroneos, P. (2004). Anti-spam initiatives in Australia. 2nd OECD Workshop on Spam - Busan, Korea - 8-9 September. [http://www.oecd.org/dataoecd/8/28/33696857.pdf]

Direct Marketing Association (2003). Definition of Spam. [http://www.dmnews.com/cgi-bin/publogin.cgi?article_id=24431]

Donaldson T. and Preston L. E. (1995), The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications, Academy of Management Review, Vol. 20, No. 1, pp. 65-91.

EU Information Society (2003). European Union launches anti-spam offensive. [http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm]

Freeman R. E. (1984), Strategic Management: A Stakeholder approach, Boston: Pitman.

FTC (2002). You've Got Spam: How to "Can" Unwanted Email.
[http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf]

Gartner Press Release (2003): 'Gartner Says Marketers Must Differentiate E-Mail Marketing From Spam.' [http://www4.gartner.com/5_about/press_releases/pr29sept2003a.jsp]

Gengler, C.E. and Thomas J.R. (1995) Consumer Understanding and Advertising Strategy: Analysis and Strategic Translation of Laddering Data. Journal of Advertising Research. July/Aug 1995. p 19-33.

Godin, Seth(1999), Permission Marketing: Turning Strangers Into Friends, and Friends into Customers, Simon & Schuster.

Graham Paul (2002). Hackers & Painters. Big Ideas from the Computer Age. O'Rielly, Inc.

Grunert, K.G. (1996). Automatic and strategic processes in advertising effects. Journal of Marketing, 60(4), 88-100.

Higa, K., Sheng, O. R.,Shin, B., and Figeuredo, A J. (2000) Understanding Relationships Among Teleworkers' E-Mail Usage, E-Mail Richness Perceptions and E-Mail Productivity Perceptions Under a Software Engineering Environment. IEEE Transactions on Engineering Management. 47(2),p.163-174.

Hoxmeier, J A. and Nie, W. (Oct-Dec2000). The Impact of Gender and Experience on User Confidence in Electronic Mail. Journal of End User Computing, 12(4) p.11-21.

Jackson, T W., Dawson, R., and Wilson, D. (Aug 2003). Understanding email interaction increases organization productivity. Communications of the ACM. 46(8), p. 80-84

Khong, D.W.K. (2004) The problem of spam law: A comment on the Malaysian Communications and Multimedia Commission's discussion paper on regulating unsolicited commercial messages. Computer Law and Security Report. 20(3).p.206-212.

Krim, J. (Mar 13 2003) Spam's Cost to Business Escalates, Washington Post, p. A01

Langford, D. (2000) Internet Ethics. Macmillan Press Ltd.

Lee, A.S. (1994). Electronic Mail as a Medium for Rich Communication: An Empirical Investigation Using Hermeneutic Interpretation. MIS Quarterly. p.142-157.

Liikanen Erkki. (2003) "Spam: European Commission goes on the offensive"
[http://www.eurunion.org/News/press/2003/2003044.htm]

McManus, D.J., Sankar, C.S., Carr, H.H., Ford, F.N. (2002): 'Intraorganizational Versus Interorganizational Uses and Benefits of Electronic Mail' Information Resources Management Journal, 15(3), p 1-13.

Meade, Joe. (2003) Spam – The death of E-mail?, Proceedings of EEMA conference, Dublin.

Milne, G.R. and Gordon, M.E.(1993), Direct mail privacy-efficiency trade-offs within an implied social contract framework, Journal of Public Policy & Marketing, 12(2), 206.

Mitchell, R, Agle,B & Wood,D (1997). Towards a theory of stakeholder identification: Defining the principle of who & what really counts, Academy of Management Review 22(4): 853-886.

Monty Python sketch (1970) [http://bau2.uibk.ac.at/sg/python/Scripts/TheSpamSketch]

Ngwenyama, O. and Lee, A. (June 2002). Communication richness in electronic mail: Critical social theory and the contextuality of meaning. MIS Quarterly Vol.21, No.2 p.145-168.

Pendharkar, P C and Young, K. (2004). The Development of a Construct for Measuring an Individual's Perceptions of Email as a Medium for Electronic Communication in Organizations. IEEE Transactions on Professional Communication. p. 130-143

Krishnamurthy, S. (2000). Spam Revisited, Quarterly Journal of E-Commerce, 1(4), 305-321.

Shiels, M. (2002). Why one spam could cost $50, BBC News, 9th April.
[http://news.bbc.co.uk/1/hi/sci/tech/1917458.stm]

Sipior, J.C., Ward, B.T. and Bonner, P.G. (Jun 2004) 'Should Spam Be On The Menu?' Communications of the ACM, 47(6), p. 59-64.

Turban, E., Lee, J., King, D. and Chung, H M (2000). Electronic Commerce: A Managerial Perspective. New Jersey: Prentice-Hall.

Weber, R. (2004). The Grim Reaper: The Curse of E-Mail. MIS Quarterly Vol. 28 No. 3, iii-xiii